DEPARTMENT OF THE AIR FORCE
HQ AIR INTELLIGENCE AGENCY

AIR INTELLIGENCE AGENCY INSTRUCTION 33-202

14 January 2000

Communications and Information

TELECOMMUNICATIONS MONITORING AND ASSESSMENT PROGRAM

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

NOTICE: This publication is available digitally on the AIA WWW site at: http://pdo.pdc.aia.af.mil/pubs.

OPR: HQ AIA/DOOF (MSgt Paul E. Clark)

Certified by: HQ AIA/DOO (Colonel Ronald L. Haygood)

Supersedes AIAI 33-202, 1 November 1998.

Pages: 11

Distribution: F

This instruction implements AFPD 33-2, *Information Protection*. It establishes procedures, responsibilities, and guidance for conducting operations according to AFI 33-219, *Telecommunications Monitoring and Assessment Program (TMAP)*. It supports Air Force Defensive Information Operations (D-IO), Defensive Counter information (DCI), and operational security (OPSEC) objectives. It applies to Air Intelligence Agency (AIA) units worldwide and AIA-gained Air Force Reserve units with TMAP missions. It does not apply to AIA-gained Air National Guard units. Refer suggested changes or conflicts to the instruction on AF Form 847, **Recommendation for Change of Publication**, to HQ AIA/DOOF, 102 Hall Blvd, Suite 229, Kelly AFB TX 78243-7029.

SUMMARY OF REVISIONS

This revision deletes mission designator abbreviations ROK for 303 IS (Republic of Korea), EDF for 381 IS (Elemendorf), OKI for 390 IS (Okinawa), and MIL for 488 IS (Mildenhall). It changes 26th Intelligence Support Flight to the 26th Intelligence Support Squadron. It adds contingency augmentation processing responsibility to the 67th Intelligence Support Flight (67 ISF), 26th Intelligence Support Squadron (26 ISS), and 692d Intelligence Support Squadron (692 ISS). Changes HQ AIA/DO duty title from Director of Information Operations to Director of Operations. Updates HQ AIA organizational office symbols. It adds the definition of a Collection Management Authority (CMA) and associated responsibilities.

Section A—Telecommunications Monitoring and Assessment Program (TMAP)

1. TMAP Unit Support and Services:

1.1. TMAP Unit Support. The AIA TMAP units support the United States Air Force major commands (MAJCOM), field operating agencies (FOA), and direct reporting units (DRU) according to AFI 33-219 and AFI 10-1101, *Operations Security*.

1.1.1. Purpose. AIA TMAP units monitor unsecure telecommunications systems to determine if they are used to transmit sensitive or classified information. Information collected is analyzed to determine if any sensitive or classified information transmitted on unsecure systems could adversely affect the United States (allied and or coalition) operations. Information is provided in near-real-time as a force protection tool or systematically collected, analyzed, put into databases, and reported to customers as long-term information liabilities.

1.1.2. Authority. Designated TMAP units conduct operations as tasked by the Directorate of Operations (HQ AIA/DO) through the 67th Intelligence Wing (67 IW) and subordinate theater groups according to this instruction. The Electronic Systems Security Assessment Centrals (ESSACs) conduct the primary operational activity in each theater of operations. The ESSACs may also conduct operations as requested by collocated and, or supported organizations. Notify the appropriate AIA group as soon as possible after receiving requests for support. The forward (Electronic Systems Security Assessment (ESSA) cells are subordinate to theater groups; they coordinate all TMAP activities with the theater ESSAC and group activities to prevent conflict in operations.

1.2. TMAP Services:

1.2.1. Services Provided. The TMAP services, consisting of monitoring telecommunications and assessing monitored data, are made available on a routine basis, during exercises, crises, contingencies, and conflicts. The monitoring and subsequent assessing of data are designed to thoroughly examine communications systems procedures associated with a specific weapon system, operation or activity, and document their vulnerability to hostile signals intelligence exploitation. Through systematic data assessment and analytical procedures, TMAP teams document the foreign hostile threat, isolate existing or potential OPSEC vulnerabilities, and identify procedures to minimize or eliminate OPSEC vulnerabilities. The TMAP is an integral part of the United States Air Force OPSEC program. Although the TMAP is considered a wartime mission, it is a very effective tool for commanders to use during day-to-day operations and exercises to identify real-world problems which can adversely affect OPSEC and the effectiveness of the warfighters. During the assessments, items such as stereotyped patterns or administrative and physical security procedures routinely surface as possible sources of intelligence losses. These items are provided as a professional courtesy to the supported commander's OPSEC office.

1.2.2. Request for TMAP Services. Organizations request TMAP services to identify information compromises that endanger personnel (force protection), identify system vulnerabilities, or evaluate OPSEC and or communications security (COMSEC) programs and posture. TMAP services include:

1.2.2.1. Stand-alone services.

1.2.2.2. Part of OPSEC Special Vulnerability Assessments (SVA).

1.2.2.3. Part of a Multi-Discipline Vulnerability Assessment (MDVA).

1.2.2.4. To support Air Force Information Protection Assessment and Assistance Program (IPAP) objectives.

2. Dissemination of Information. Information disseminated on planned TMAP assessment missions is limited to a need-to-know basis to ensure mission effectiveness is not jeopardized. Handle information on planned missions through the designated point of contact.

3. Disposition of Information. Materials collected or developed during operations are protected and handled according to DoD 5200.1-R, *Information Security Program*, AFMAN 37-139, *Records Disposition Schedule*, table 33-24, and applicable security classification guides. Store information according to guidelines for the applicable level of classification or handling instructions to prevent unauthorized access.

4. Other Agency Support. Occasionally, assessment resources support Joint COMSEC Monitoring Activity (JCMA) requirements. When a unified commander-in-chief or Joint Task Force commander designates JCMA as executive agent for an operation or exercise, JCMA coordinates all monitoring activities with AIA TMAP units. If designated executive agent authority, JCMA coordinates the collection effort of the SCE assigned to the service component of the unified command to ensure the monitoring is focused on priorities of the joint commander. If granted executive agent authority, JCMA manages the efforts of AIA TMAP units. When supporting JCMA efforts, AIA TMAP units provide the finished products, such as reports, to JCMA to compile into a joint report. AIA TMAP units prepare reports in the format of a Tactical Advisory (TACAD), Daily Summary (DASUM), Periodic Analytical Summary, or a Final Analytical Report as specified in the Joint Staff, National Security Agency (NSA) Memorandum of Agreement (MOA). A copy of the current MOA is provided to all operational elements by the Current Operations Division (HQ AIA/DOOF).

Section B—Telecommunications Monitoring and Assessment Program Procedures

5. Establishing a Mission:

5.1. Mission Designators. The 67 IW or the appropriate group assigns mission designators to all official requests tasked, whether or not the support is provided. Project or mission designators consist of three-letter abbreviations with one-up numbers followed by the fiscal year the mission is tasked. Use 01 through 99 for missions tasked annually. Use 100 through 199 for out-of-cycle mission requests.

5.2. Mission designator abbreviations include:

67 IW	AIA
ESSAC-CONUS (Continental United States)	CON
ESSAC-Europe	EUR
ESSAC-Pacific	PAC
25 IS (Hurlburt Field)	HUR
710 IF (Brooks)	RFB
610 IF (Offutt)	RFO

5.2.1. Use a 67 IW mission designator when two or more theaters are involved in a specific tasking. The 67 IW designates an executive agent for the mission.

6. Notice and Consent:

6.1. Requirements. Notice and consent requirements for telecommunications monitoring are specified in AFI 33-219. AIA units do not conduct telecommunications monitor missions at any location unless these provisions are met. Do not misconstrue TMAP efforts in any way as intelligence gathering activities. The Secretary of the Air Force, General Counsel (SAF/GC) certification continues in effect for a unit being monitored when it deploys, even if the unit deploys to a base or location which is not certified.

6.2. Authorizing TMAP Operations. HQ AIA/DO obtains a legal review before authorizing TMAP operations. During United States Air Force-only monitoring, a current and unexpired SAF/GC certification is proof of the legality of the monitoring, and no further review is needed. During Joint Service monitoring, the JCMA authorization may be accepted and no further legal review is needed.

7. TMAP Procedures:

7.1. Telecommunications Monitored. For telecommunications monitored, the data that is collected using automated collection systems is reviewed, the mission data is separated, compiled and, or summarized using applicable automated systems software and configuration controls. The data collected is maintained magnetically unless it is determined to be personal privacy information (PPI). Maintaining PPI is of no operational value and is prohibited according to AFI 33-219. Immediately destroy PPI and prohibited data upon recognition according to AFI 33-219, section E. Also destroy nonoperational data as soon as operationally feasible, but no later than 90 days from the issuance of a final report for which the information was originally collected.

7.2. Obtaining Internet Protocol (IP). Provisions for collecting computer-to-computer data are outlined in AFI 33-219 and this instruction. The TMAP units obtain necessary IP addresses from mission points of contact to ensure only authorized addresses are monitored. Insertion for monitoring is on the Air Force side of any router only. Monitoring operations do not attempt to capture stored data resident on personal computers. Key word searches are used to obtain operational data and attachments. Monitored data is reviewed expeditiously and handled according to AFI 33-219 and this instruction.

7.3. Releasing Information. For releasing sanitized and unsanitized transcripts, the information acquired in the course of a TMAP mission is released outside of TMAP units only after following the provisions of AFI 33-219 and this instruction. Information collected using the facsimile and electronic-mail collection systems are released in a summary format only. The information collected is sanitized to remove all names and other identifying data. For releasing unsanitized data, follow provisions listed in AFI 33-219. In addition, prepare a cover letter and forward the unsanitized monitored data to HQ AIA/DO for approval. The release of an unsanitized reproduction of a collected communication is only conducted with written approval of HQ AIA/DO.

7.4. Transcripts. Use the format described in the AIA 1N6 Study Guide, when releasing sanitized or unsanitized transcripts. Use the formats developed locally for other transcripts and analytical notes as the basis for report generation. TMAP units must maintain monitored data used as a basis for a reportable item for up to 90 days after final report distribution. If necessary, this allows customers to obtain sanitized or unsanitized transcripts to assist in correcting security problems.

7.4.1. Sanitized Transcripts. If prepared electronically, include an introductory paragraph. Reference all previous correspondence relating to the release of the transcript; also, identify the dates and times of the conversation, location or locations involved, mission number, and tasking author-

ity. Include an explanatory paragraph on the procedures to be followed to obtain a complete transcript if the situation warrants further action. Mark the transcripts with the statement in figure 1.

7.4.2. Unsanitized Transcripts. After reviewing sanitized transcripts, the consumer may request unsanitized transcripts by certifying, in writing, to HQ AIA/DO, that a security violation has occurred. HQ AIA/DO will coordinate the request with Staff Judge Advocate (HQ AIA/JA) and provide direction to the TMAP element for release decision according to AFI 33-219. When making the request:

7.4.2.1. Send the transcript to HQ AIA/DO with a cover letter. Reference all previous correspondence relating to the project or mission number, dates, and times of the conversation, locations involved, and the telephone circuit or radio frequency. Include all information necessary for clarity and explain any items which may not be obvious to the reader.

7.4.2.2. Mark transcripts with the appropriate, overall classification and include the statement:

Figure 1. Statement for Transcript.

"Access to this transcript is for evaluation purposes only. The number of personnel provided access should be kept to the absolute minimum necessary for a complete evaluation."

7.4.3. Classifying Transcripts. Classify all transcripts (sanitized or unsanitized) according to content. As a minimum, mark transcripts FOR OFFICIAL USE ONLY.

8. Handling and Reporting TMAP Derived Information:

8.1. Producing TMAP Reports. TMAP reporting must be timely, accurate, and comprehensive. Assessment reports are highly visible at all levels of command within the Air Force. Clearly identify each report as a TMAP product and prominently display an access clause at the beginning of the report. In capital letters state: THE INFORMATION IN THIS REPORT IS USED ONLY FOR OFFICIAL UNITED STATES GOVERNMENT TMAP PURPOSES. Mission supervisors determine the precedence of a telecommunications monitoring report (TMR) based upon the presumed urgency and significance of the information being reported.

8.2. Telecommunications Assessment Report (TAR). The TAR is issued to the customer no later than 30 calendar days after mission completion. If for some reason this is not accomplished, an interim message is sent to the customer and the appropriate group stating the cause and the projected report completion date. All TMAP missions require a final report. If the customer requests a verbal out brief, a hard copy or magnetic media version of the out brief is constructed as a record for management and quality control. If additional or refined information is developed through more in-depth analysis after issuing the original TAR, send it to the same addressees as the original report. When the team is physically separated from the addressee, daily or weekly summary reports are normally issued by electrical means at routine precedence.

8.2.1. Threat Assessments. Upon receipt of the units vulnerability and or threat assessment, evaluate the assessment and use it to tailor your reporting. Include the significant and specific threat to susceptibility or vulnerability of the monitored communications in the TAR. If it will allow wider distribution of the basic report, you may send this information separately.

8.2.2. Online Reporting of TMAP Information. When Secure Internet Protocol Network (SIPRNET) or Intelink methods are developed to distribute TMAP-related information, follow the provisions of AFI 33-219 and this instruction. Access controls are developed to ensure only those authorized organizations are allowed to review TMAP information.

8.3. Emergency, Significant Crime and Fraud, Waste, and Abuse Information:

8.3.1. Emergency. According to AFI 33-219, paragraph 24.5, immediate notification is authorized when information acquired inadvertently during the course of an authorized TMAP operation reveals an emergency situation or situation threatening death or grievous bodily harm.

8.3.2. Crime. Information acquired inadvertently during the course of an authorized TMAP operation and relates directly to a significant crime except those communications protected by attorney-client privilege, is referred to the military commander, Air Force Office of Special Investigations (AFOSI), or law enforcement agency having appropriate jurisdiction over the unit being monitored.

8.3.2.1. A significant crime is one for which the *Manual for Courts-Martial, United States* (as amended) lists a Dishonorable Discharge as part of the maximum punishment. Examples include robbery, extortion, indecent assault, arson, desertion, assaulting an officer, espionage, murder, manslaughter, burglary, kidnapping, obstruction of justice, communication of a bomb threat or hoax, wrongful use of certain controlled substances, and others. Consult the staff judge advocate for advice on specific cases.

8.3.2.2. Attorney-client privilege consists of confidential communication between attorney and client regarding a matter on which the client has sought the attorney's professional advice and assistance. The phone line of the base legal office and Area Defense Counsel is identified and avoided, wherever possible. Refer questions on attorney-client privilege to the staff judge advocate.

8.3.3. Fraud, Waste, and Abuse Information. Significant fraud, waste, and abuse information is reported to the military commander, Inspector General, AFOSI detachment, or law enforcement agency with jurisdiction over the unit where the monitoring occurred. Fraud, waste, and abuse information is defined in AFI 90-301, *Inspector General Complaints*, attachment 1.

8.3.3.1. Fraud is any intentional deception designed to unlawfully deprive the Air Force resources including misuse of computers.

8.3.3.2. Waste is extravagant, careless or needless expenditure of Air Force funds for the consumption of Air Force property.

8.3.3.3. Abuse, according to AFI 33-129, *Transmission of Information via the Internet*, paragraph 6, contains specific prohibitions including use of Air Force computers for unauthorized commercial or financial activities, chain letters, solicitation of financial ventures, hate literature, pornography. Use of Air Force computers is also subject to the rules of ethics in DoD 5500.7 and prohibitions against unauthorized computer games.

8.3.4. TMAP Operations Results. See AFI 33-219, paragraph 25, for further use of TMAP operations results. The TMAP units promptly notify HQ AIA/DO and HQ AIA/JA of any referrals. HQ AIA/JA notifies SAF/GC.

8.4. Security Classification Guidance for TMAP Reports:

8.4.1. TMAP units work diligently with supported commanders, designated POCs, and OPSEC officers to obtain current classification guides and critical information listings to aid in applying derivative classifications to TMAP-gathered data summarized in a report. These documents are available for nearly all Air Force operations. If available, classification guidance provided by supported agencies are used. A report of no findings is unclassified.

8.4.2. According to Chairman Joint Chiefs of Staff Instruction (CJCSI) 6510.01B, all reports, logs, and materials produced in the course of COMSEC monitoring are afforded protection commensurate with the classification of the information and the sensitivity of the monitored activity. Reports or materials produced from COMSEC monitoring which identify security weaknesses of the monitored activity are classified at least CONFIDENTIAL and downgraded to UNCLASSIFIED when security weaknesses are corrected.

8.5. Recorded Magnetic Media. Label recorded magnetic media FOR OFFICIAL USE ONLY unless a specific higher level of classified information is knowingly recorded. Label and safeguard information according to DOD 5200.1-R. Restrict access to recorded TMAP material to authorized personnel. Raw monitored data is reviewed expeditiously; nonoperational data is discarded as soon as operationally feasible. Information used for reporting purposes are maintained within databases adhering to the purge requirements of the databases. Periodic reviews are conducted to ensure accuracy and currency. Reportable information not in a database due to special access programs (SAP), is maintained according to governing instructions related to the supported SAP. Information is not maintained without adequate controls in place to ensure that the information is protected from unauthorized access.

8.6. Quality Control (QC). QC is an integral part of accomplishing and managing the mission and is necessary to ensure all aspects of TMAP operations are the most professional possible. QC checks identify strengths and weaknesses of training processes, ensures customers receive professional and quality products, and serves as a feedback tool through trends analysis to share training strengths and correct training deficiencies. HQ AIA reviews QC evaluation reports during staff assistance visits and through the Inspector General process to ensure compliance with the appropriate instructions and pamphlets. TMAP units establish procedures for an aggressive QC program. At a minimum, procedures contain a sample evaluation of an individual's products, and trends analysis reporting at least semiannually. Documentation records of evaluations are maintained and trend reports are coordinated with formal training programs to enhance the training process.

8.7. SENSOR QUEST Analytical Databases. General telecommunications assessment reference information is essential to effective monitor operations. It provides TMAP personnel with the knowledge needed for a given mission. To support this program and ensure the analyst reference data files within their theaters are current and essential, TMAP units must ensure that personnel review all reference materials regularly and establish procedures to ensure the currency of analyst reference data files. The TMAP units ensure that information on specific individuals is not maintained in the database.

Section C—Responsibilities

9. HQ AIA/DO:

9.1. Ensures TMAP services are provided to support national and United States Air Force goals. HQ AIA/DOO markets TMAP services to include soliciting annual TMAP requirements from USAF customers.

9.2. Provides TMAP policy guidance to AIA and AFRC assessment field elements.

9.3. Assists in coordinating 610th Intelligence Flight (610 IF) and 710th Intelligence Flight (710 IF) tasking with the Assistant Director of Intelligence (HQ AFRC/ADI) or as stated in current agreements with HQ AFRC.

9.4. Provides staff assistance and augmentation to AIA and AFRC reserve elements when requested.

9.5. Coordinates biennial Notice and Consent requirements with the Air Force Communications Agency.

9.6. Directs and coordinates all TMAP contingency tasking in support of DoD goals according to AFMAN 10-401, *Operation Plan and Concept Plan Development*.

10. The Air Force Information Warfare Center, Directorate of Operations Support (AFIWC/OS):

10.1. Provides communications-electronics threat, vulnerability data, and source lists to TMAP units for use in preparing specific threat briefings and assessments according to AFI 33-219.

10.2. Provides technical support and information as required by AIA or 67 IW.

10.3. Coordinates support requirements for MDVAs with HQ AIA, 67 IW, and appropriate theater groups. All coordination and details concerning MDVAs are considered sensitive, at a minimum, and requires special handling restrictions. Use of secure communications and strict need-to-know are crucial to effectiveness of the MDVA and the operation supported.

11. The 67 IW:

11.1. Provides operational and technical guidance and day-to-day oversight for TMAP units.

11.2. Monitors customer support and satisfaction database developed by TMAP units and provides data to HQ AIA upon request.

11.3. Consolidates annual TMAP tasking requirements and coordinates scheduling with subordinate units.

11.4. Develops and submits program objective memorandum (POM) submissions for acquisition, sustainment, and life-cycle support to HQ AIA as needed.

11.5. Develops new operational concepts in the expanding field of telecommunications assessment operations. Validates requirements with HQ AIA/DO for system upgrade and modification.

11.6. Researches and expands ESSA initiatives to support the United States Air Force D-IO, DCI, OPSEC, and IP goals.

11.7. Maintains personnel accounting database by mission areas and provides data to HQ AIA upon request.

12. The 67th Intelligence Support Flight (67 ISF), 26th Intelligence Support Squadron (26 ISS), and 692d Intelligence Support Squadron (692 ISS). Each unit:

12.1. Provides oversight and advocacy for subordinate ESSACs and TMAP units to include 1N6X1 personnel assigned to information operations detachments (IOD).

12.2. Prevent conflicts in annual and or out-of-cycle tasking for subordinate units.

12.3. Serves as focal point for respective theater short-notice requirements.

12.4. Facilitates resolution of shortfalls in resources to include manpower, expertise, equipment, or funding with higher headquarters for subordinate units.

12.5. Monitors customer support and satisfaction database developed by the ESSACs and provides data to higher headquarters upon request.

12.6. Functions as 67 IW primary interface with MAJCOMs for theater operations and "reach back."

12.7. Develops requirements for command resources with Joint Operational Planning Execution System (JOPES).

Requests contingency augmentation from HQ AIA/DO in accordance with AFMAN 10-401, *Operations Plans and Concept Plans Development and Execution.*

13. ESSACs:

13.1. Conduct ESSA operations to support TMAP objectives. ESSA operations include telecommunications monitoring for telephone, cellular telephone, radio, data modem and, or facsimile, electronic mail (e-mail), computer-to-computer, and Unclassified Internet Protocol Router Network (NIPRNET) previously known as military network (MILNET) open source.

13.2. Plan, schedule, and conduct TMAP operations in direct response to theater requirements and conduct missions in-garrison through remote operations, or by sending appropriate resources on temporary duty. The scope of remoting depends on a variety of factors. Theses factors include objectives of the mission, the level of support available at forward ESSA cells, and the availability of connectivity at the mission site.

13.3. Operate 24-hour capable analysis and reporting cell for theater TMAP requirements.

13.4. Provide technical expertise and augmentation support to theater information protection (IP) managers as required. Work closely with MAJCOM IP and OPSEC program managers to test, validate, and integrate emerging AIA IP technologies and methodologies to support IP and OPSEC programs.

13.5. Immediately advise the appropriate AIA intermediate headquarters when manpower, expertise, equipment, or funding is not available at the unit to meet tasking requirements. AFRC units notify HQ AFRC/ADI and 10 AF/DOI.

13.6. Advise the appropriate intermediate AIA headquarters of any requests for support received directly from a MAJCOM or FOA.

13.7. Develop folders or electronic files for all tasked assessment projects and missions; include tasking, coordination, general correspondence, and reports issued.

13.8. Develop project and mission checklists to ensure all required actions are performed.

13.9. Establish procedures to ensure the commander or senior official of the organization monitored, is aware of the impending mission prior to commencing operations and offer briefings through your mission POC.

13.10. Notify the AIA-unit commander assigned to the installation and, or area when a TMAP team is working in the vicinity. With knowledge of the team's presence, the AIA-assigned unit commander can provide liaison support for the mission, if it becomes necessary. When supporting MDVAs, offer briefings through your mission POC.

13.11. Produce threat assessments or briefings as required to support the mission and request assistance from AFIWC/OS as required. Maintain a current database of threat information and identify sources for threat data.

13.12. Maintain a mission support database.

13.13. Establish procedures for, and maintain a quality control program. At a minimum, the program includes the elements outlined in this instruction, and ensures recurring trends are identified and used to enhance training.

13.14. Collect data to identify trend analysis of information liabilities to enhance OPSEC education and awareness.

13.15. Notify the local AFOSI unit that an assessment team is working in the area. This action is required in the event emergency or other reporting becomes necessary according to AFI 33-219. When supporting MDVAs, coordinates AFOSI briefings with the mission point of contact.

13.16. Utilize the AIA 1N6 Study Guide to support operations training and submit recommended changes to the intermediate headquarters at 67 IW/DOT and HQ AIA/DOOF.

13.17. Develop local operating instructions as needed to support operations.

14. The 1N6X1 Personnel Assigned to Forward ESSA Cells:

14.1. Works with collocated MAJCOM or Numbered Air Force (NAF) war planners to develop input for TMAP wartime Operations Plans (OPlans) requirements.

14.2. Works with MAJCOM or NAF OPSEC and deception managers to develop feedback mechanisms to ensure TMAP services and products adequately support their programs.

14.3. Works with host base communication squadron to facilitate TMAP workspace and connectivity requirements for supporting TMAP units.

14.4. Assists theater ESSAC with data collection in their Area of Responsibility (AOR).

15. Collection Management Authority (CMA). When two or more ESSACs are involved in the processing of

data for a specific mission, the lead ESSAC is designated the CMA. The CMA resides with the ESSAC Area of Responsibility (AOR) where the mission is occurring; that is, ESSAC-PAC (Pacific theater), ESSAC-EUR (European theater), and ESSAC-CON (Continental United States). CMA responsibilities include:

15.1. Establishing a Monitor Management Plan (MMP) which includes at a minimum:

15.1.1. Monitoring site locations and resource composition.

15.1.2. Reporting requirements for TMAP elements and unique reporting situations.

15.1.3. Setting data transfer schedules.

15.1.4. Establishing data disposition procedures at mission termination.

15.2. Submitting MMP through theater intermediate headquarters for coordination with 67 IW for assignment of ESSAC support and publication.

LYNN W. WAKEFIELD, Colonel, USAF
Director of Operations